11-12

Территориальный фонд обязательного медицинского страхования Смоленской области

ПРИКАЗ

«16» 12 2014г. № 226

г. Смоленск

Об утверждении политики в отношении обработки и обеспечения безопасности персональных данных и положения о порядке обработки и обеспечения безопасности персональных данных

В целях исполнения положений Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных» по порядку обработки и обеспечению безопасности персональных данных, обрабатываемых в Территориальном фонде обязательного медицинского страхования Смоленской области

п р и к а з ы в а ю:

1. Утвердить прилагаемую «Политику в отношении обработки и обеспечения безопасности персональных данных Территориального фонда обязательного медицинского страхования Смоленской области» (далее – Политика) (Приложение №1).

2. Ознакомить под роспись работников Территориального фонда обязательного медицинского страхования Смоленской области, допущенных к обработке персональных данных, с содержанием Политики.

3. Опубликовать Политику в сети Интернет на официальном сайте Территориального фонда обязательного медицинского страхования Смоленской области.

4. Обработку персональных данных в Территориальном фонде обязательного медицинского страхования Смоленской области осуществлять в порядке определенном в Политике.

6. Приказ довести до лиц, допущенных в обработке персональных данных

7. Контроль за исполнением приказа оставляю за собой.

Директор Бельков А.В.

Приложение №1

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Территориального фонда обязательного медицинского страхования Смоленской области

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Политика защиты персональных данных (далее – Политика) разработана на основании ст. 24 Конституции РФ, главы 14 Трудового Кодекса РФ, Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., ГОСТ Р ИСО/МЭК 27002-2012 «Методы и средства обеспечения безопасности», Приказа ФСТЭК России № 21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации от 21 марта 2012 г. N 211 г. Москва "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

1.2. Настоящая Политика утверждается приказом директора Территориального фонда обязательного медицинского страхования Смоленской области.

1.3. Настоящая Политика определяет:

- порядок обработки (сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления доступа), обезличивания, блокирования, удаления, уничтожения) персональных данных в Территориальном фонде обязательного медицинского страхования Смоленской области (далее – ТФОМС);

- порядок обеспечения защиты прав и свобод субъектов персональных данных при обработке их персональных данных с использованием средств автоматизации или без использования таких средств, а также устанавливает ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих обработку и защиту персональных данных.

Целью настоящей Политики является обеспечение безопасности объектов защиты ТФОМС от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование,

копирование, распространение персональных данных, а также иных несанкционированных действий.

1.5. Для целей настоящей Политики используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

1.6. В настоящей Политике используются следующие обозначения и сокращения:

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

НСД – несанкционированный доступ

ПДн – персональные данные

СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных

2 ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящей Политики распространяются на всех работников ТФОМС, а также всех прочих лиц (имеющих санкционированный доступ информационным системам и ресурсам ТФОМС (исполнители государственных контрактов, аудиторы, эксперты и т.п.).

3 ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основной целью обеспечения безопасности персональных данных является минимизация ущерба (как непосредственного, так и опосредованного), возникающего вследствие возможной реализации угроз безопасности персональных данных.

Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту персональных данных и может проявляться в виде:

- нанесения вреда здоровью субъекта персональных данных;
- незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;
- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием персональных данных;
- нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности государственных органов, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с персональными данными.

Основной задачей обеспечения безопасности персональных данных, при их обработке в ТФОМС, является предотвращение утечки персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения

4 ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Состав персональных данных

Состав персональных данных и ИСПДн, подлежащих защите, определяется в ходе проведения обследования информационных потоков в ТФОМС и отражается в «*Сводном перечне персональных данных, подлежащих защите*».

4.2.Категории субъектов персональных данных

В ТФОМС обрабатываются персональные данные следующих субъектов:

1) Работники ТФОМС, обработка персональных данных которых осуществляется в целях выполнения положений Трудового Кодекса РФ.

2) Граждане, обработка персональных данных которых осуществляется в целях выполнения положений Федерального закона № 326 – ФЗ от 29.11.2010 « Об обязательном медицинском страховании в Российской Федерации».

4.3. Цели обработки персональных данных

В основе определения целей обработки персональных данных лежит принцип законности их обработки.

Целями обработки персональных данных работников являются содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества.

Цели обработки персональных данные в ИСПДн ТФОМС определены ст. 34 Федерального закона № 326 – ФЗ от 29.11.2010 « Об обязательном медицинском страховании в Российской Федерации» и Правилами обязательного медицинского страхования, утвержденных приказом Министерства здравоохранения и социального развития Российской Федерации от 28.02.2011 N 158н

Целями обработки персональных данных граждан является:

1. Ведение персонифицированного учета сведений о застрахованных лицах в форме регионального сегмента единого регистра застрахованных лиц.

2. Контроль за использование средств обязательного медицинского страхования на территории РФ, обеспечение прав граждан в сфере обязательного медицинского страхования на территории субъекта РФ.

3. Осуществление расчетов за медицинскую помощь, оказанную застрахованным лицам за пределами субъекта Российской федерации, на территории которого выдан полис обязательного медицинского страхования.

4. Ведение единого реестра страхователей.

5. Ведение территориального реестра экспертов качества медицинской помощи в соответствии с порядком организации и проведения контроля объемов, сроков, качества и условий предоставления медицинской помощи.

6. Ведение информационного сопровождения застрахованных лиц при организации оказания им медицинской помощи страховыми медицинскими организациями.

При определении целей обработки персональных данных иных категорий субъектов персональных данных, необходимо соблюдать законы и иные нормативно-правовые акты.

4.4. Состав персональных данных субъектов персональных данных

Состав персональных данных должен соответствовать принципу их достаточности для достижения целей обработки (персональные данные не должны быть избыточными по отношению к целям обработки).

4.5. Характеристики безопасности персональных данных

Персональные данные, обрабатываемые в информационных системах ТФОМС, обладают как минимум свойством конфиденциальности.

Данная характеристика не являются исчерпывающей, в дополнение к ней могут рассматриваться и другие характеристики безопасности. В частности, к таким характеристикам относятся: целостность, доступность.

Для обеспечения заданных характеристик безопасности персональных данных в ТФОМС реализован минимальный и достаточный набор организационно-технических мер.

5 ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПД И ИСПДн

Построение СЗПДн в ТФОМС и ее функционирование осуществляется в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность и адекватность;
- персональная ответственность;
- минимизация полномочий;
- гибкость;
- открытость алгоритмов и механизмов защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- знание работников;
- наблюдаемость и оцениваемость;
- обязательность контроля и оценки.

5.1. Законность

Защита ПДн в ИСПДн ТФОМС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите ПДн и учитывает лучшие мировые практики.

5.2. Системность

Системный подход к построению СЗПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ТФОМС.

5.3. Комплексность

Безопасность ПДн обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер, реализованных ТФОМС.

Применение различных средств и технологий защиты информации обеспечивает предотвращение все существенных (значимых) каналов реализации угроз безопасности ПДн.

СЗПДн строится с учетом не только всех известных каналов проникновения и несанкционированного доступа (далее – НСД) к ПДн, но и с учетом возможности повышения уровня защиты по мере выявления новых источников УБПДн, развития способов и средств их реализации в ИСПДн.

СЗПДн ТФОМС строится на основе единой технической политики, с использованием функциональных возможностей информационных технологий, реализованных в информационной системе и имеющихся систем и средств защиты в соответствии с разработанными типовыми моделями угроз и профилями защиты. При создании СЗПДн могут использоваться системы и средства защиты информации, используемые в организации для обеспечения безопасности иной конфиденциальной информации.

5.4. Непрерывность

Защита ПДн обеспечивается на всех технологических этапах обработки ПДн и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

5.5. Своевременность

Принимаемые меры по обеспечению безопасности ПДн носят упреждающий характер.

ТФОМС принимает необходимые меры по защите ПДн до начала обработки ПДн, которые должны обеспечить надлежащий уровень безопасности ПДн.

СЗПДн разрабатывается одновременно с разработкой и развитием ИСПДн ТФОМС, что позволяет учитывать требования по безопасности ПДн при проектировании и модернизации ИСПДн.

5.6. Преемственность и непрерывность совершенствования

Предполагают постоянное совершенствование мер и средств защиты ПДн на основе результатов анализа функционирования ИСПДн и СЗПДн с учетом выявления новых способов и средств реализации УБПДн, отечественного и зарубежного положительного опыта в сфере защиты информации.

ТФОМС определяет действия, необходимые для устранения причин потенциальных несоответствий требованиям по безопасности ПДн с целью предотвратить их повторное появление.

5.7. Разумная достаточность и адекватность

Состояние и стоимость реализации мер защиты должно быть соизмеримы с рисками, связанными с обработкой и характером защищаемых ПДн.

Анализ рисков нарушения безопасности ПДн проводится в целях определения влияния системы защиты информации на вероятность реализации угроз безопасности ПДн с учетом уязвимостей (дефектов) ИТ-инфраструктуры ТФОМС.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики и производительность ИСПДн ТФОМС.

5.8. Персональная ответственность

Ответственность за обеспечение безопасности ПДн и ИСПДн ТФОМС возлагается на каждого работника в пределах его полномочий.

Распределение обязанностей и полномочий работников ТФОМС позволяет обеспечить выявление виновных лиц в случаях нарушения безопасности ПДн.

Роли и обязанности работников определены и документально подтверждены в соответствии с организационной политикой в области защиты информации.

5.9. Минимизация полномочий

Предоставление и использование прав доступа к ПДн ограничено и управляемо.

Пользователям предоставляются минимально необходимые права доступа к ПДн и ИСПДн только в соответствии с производственной необходимостью.

Доступ к ПДн предоставляется только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

Пользователю запрещены все операции с ПДн за исключением тех, которые разрешены явно.

5.10. Гибкость

В процессе функционирования ИСПДн могут меняться ее характеристики, а также объем и категория обрабатываемых ТФОМС ПДн.

Для обеспечения возможности варьирования уровня защищенности ПДн, СЗПДн ТФОМС обладает определенной гибкостью.

5.11. Открытость алгоритмов и механизмов защиты

Защита ПДн не должна осуществляться только за счет сокрытия структуры, технологий и алгоритмов функционирования СЗПДн.

Знание указанных характеристик СЗПДн не должно давать возможности преодоления защиты возможными нарушителями безопасности ПДн, включая разработчиков средств защиты.

5.12. Научная обоснованность и техническая реализуемость

Уровень рекомендаций и требований по защите ПДн соответствует имеющемуся уровню развития информационных технологий и средств защиты информации.

При создании и эксплуатации СЗПДн используются лучшие современные отечественные и зарубежные технические решения и практику защиты информации.

5.13. Специализация и профессионализм

Реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляется профессионально подготовленными специалистами ТФОМС или же специалистами организации, лицензиата ФСТЭК России и ФСБ России, на основании государственного контракта или договора гражданско-правового характера.

5.14. Знание своих работников

ТФОМС реализует кадровую политику (тщательный подбор персонала и мотивация работников), позволяющую исключить или минимизировать возможность нарушения безопасности ПДн своими работниками.

5.15. Наблюдаемость и оцениваемость обеспечения безопасности персональных данных

Предлагаемые ТФОМС меры по обеспечению безопасности ПДн спланированы так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен федеральными органами исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

5.16. Обязательность контроля и оценки

Неотъемлемой частью работ по защите ПДн является оценка эффективности системы защиты.

С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн в ТФОМС определены процедуры для постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

6 ОБЩИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Классификация методов обеспечения безопасности персональных данных

Методы обеспечения безопасности ПДн разделяются на:

- административно-правовые;
- организационно-технические;
- физические.

По времени применения методы обеспечения безопасности ПДн разделяются на:

- превентивные;
- восстановительные.

6.2. Административно-правовые методы

К административно-правовым методам защиты относятся нормы действующего законодательства и внутренние организационно-распорядительные документы ТФОМС, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе обработки и использования ПДн, а также устанавливающие ответственность за нарушения этих правил, препятствуя неправомерному использованию ПДн и являющиеся сдерживающим фактором для реализации угроз безопасности потенциальными нарушителями.

Основными направлениями этой деятельности ТФОМС являются:

- разработка, внесение изменений и дополнений в политику информационной безопасности в части защиты ПДн и поддерживающие ее документы;
- регламентация процессов обработки ПДн;
- определение ответственности за нарушения в области обеспечения безопасности ПДн;
- назначение и подготовка должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн;
- закрепление в должностных инструкциях установленного разграничения полномочий в области обеспечения безопасности ПДн;
- разработка и принятие документов, устанавливающих ответственность структурных подразделений и сотрудников, а также взаимодействующих юридических лиц, за несанкционированный доступ к ПДн, противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверных ПДн, противоправное их раскрытие или использование в преступных и корыстных целях;
- контроль знания и соблюдения пользователями ИСПДн, требований организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;

- проведение постоянного анализа эффективности и достаточности принимаемых мер и применяемых средств защиты ПДн, разработка и реализация предложений по совершенствованию СЗПДн;
- проведение аттестационных мероприятий для подтверждения соответствия принятых мер требованиям законодательства в области защиты персональных данных.

6.3. Организационно-технические методы

Организационно-технические методы защиты основаны на использовании организационных мер, различных программных, аппаратных и программно - аппаратных средств, входящих в состав СЗПДн и выполняющих функции защиты информации, направленных на решение следующих задач:

- строгий учет всех подлежащих защите ресурсов (персональных данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
- предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременного обнаружения фактов НСД к ПДн;
- недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянного контроля за обеспечением уровня защищенности ПДн.

6.4. Физические методы

Физические методы защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

6.5. Превентивные методы

Превентивные методы противодействия угрозам безопасности ПДн осуществляются на основе эффективного применения в процессе эксплуатации ИСПДн комплекса организационных, технических и технологических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИСПДн.

Организационные мероприятия по обеспечению безопасности ПДн являются мероприятиями общего характера по организации деятельности персонала, эксплуатирующего ИСПДн, порядку применения информационных технологий в зданиях и сооружениях, систематическому применению мер по недопущению вывода ИСПДн из строя.

Технические мероприятия по обеспечению безопасности ПДн заключаются в обслуживании, поддержании и управлении требуемым составом технических средств, обеспечивающих обработку ПДн в защищенном режиме.

Технологические мероприятия по обеспечению безопасности ПДн направлены на правильную реализацию функций и заданных алгоритмов работы ИСПДн, технологий обработки ПДн и защиту программ и ПДн от преднамеренных и непреднамеренных нарушений.

6.6. Восстановительные методы

Планирование восстановительных методов определяется системой документов, устанавливающих требования к обязательным мероприятиям, проводимым заблаговременно и после возникновения нарушений, угрожающих штатному функционированию ИСПДн.

6.7. Основные этапы работ по обеспечению безопасности персональных данных

В число основных этапов работ по обеспечению безопасности персональных данных входят, в частности, следующие:

- определение объектов защиты;
- установление целей защиты объектов защиты;
- определение угроз объектам защиты;
- установление требований к системе защиты персональных данных;
- определение порядка контроля и надзора.

Основным объектом защиты являются персональные данные.

Персональные данные могут иметь различные формы представления (бумажная, файлы, записи и поля записей баз данных, электромагнитные волны и поля, излучения и т.д.), каждая из которых является объектом защиты.

Формы представления персональных данных связаны с различными ресурсами информационной системы персональных данных, которые в свою очередь могут порождать объекты защиты.

Используемые в информационной системе персональных данных средства защиты информации являются объектами защиты.

Информация о методах и средствах обеспечения безопасности персональных данных содержит сведения, которые являются объектами защиты, в частности, к таким объектам могут быть обнесены парольная и аутентифицирующая информация, ключевая информация

Установление целей защиты объектов защиты связано с установлением характеристик безопасности для каждого из определенных объектов защиты.

Определение угроз объектам защиты проводится путем формирования модели угроз и модели нарушителя. При этом модель нарушителя формируется как

составная часть модели угроз, определяющая возможные специфические угрозы – атаки.

Установление требований к системе защиты персональных данных основано на формировании моделей угроз и нарушителя.

В первую очередь устанавливаются общие требования к организационным мерам.

Далее на основе моделей угроз и нарушителя, сформированных в соответствии с нормативными и методическими документами ФСТЭК России и ФСБ России, определяются требования к средствам защиты информации, а также требования к поддерживающим эти средства организационным мерам.

Процесс формирования требований к системе защиты персональных данных заканчивается, если выполнение установленных требований нейтрализует все угрозы, перечисленные в моделях угроз и нарушителя.

7 ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн ТФОМС назначается должностное лицо, ответственное за обеспечение безопасности ПДн.

Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

- мероприятия по организации обеспечения безопасности ПДн, включая классификацию ИСПДн;
- мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;
- мероприятия по защите ПДн от несанкционированного доступа и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн;
- мероприятия по организации криптографической защиты каналов связи.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой СЗПДн. Структура, состав и основные функции СЗПДн определяются с учетом требуемого уровня защищенности ИСПДн.

Перечень реализуемых мероприятий по защите ПДн при их обработке в специальных ИСПДн определяется на основании анализа актуальности угроз, рисков безопасности ПДн, в соответствии с нормативными и методическим документами ФСБ России и ФСТЭК России.

ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным информационным системам, поэтому целесообразно при их защите максимально использовать традиционные подходы к технической защите информации в автоматизированных системах.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

В соответствии с нормативными документами Федеральной службы по техническому и экспортному контролю:

- осуществляется обеспечение защиты (некриптографическими методами) информации;
- проводятся мероприятия по предотвращению утечки информации по техническим каналам;
- проводятся мероприятия по предотвращению несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, и блокирования доступа к ней.

В соответствии с нормативными документами Федеральной службы безопасности Российской Федерации:

- устанавливаются особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах;
- проводятся мероприятия по обнаружению компьютерных атак.

Мероприятия по обеспечению безопасности ПДн включают в себя:

- управление доступом:
  - идентификация и аутентификация;
  - физическая защита;
- регистрацию и учет;
- обеспечение конфиденциальности;
- обеспечение целостности;
- обеспечение доступности;
- обеспечение достоверности (аутентичности);
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия;
- анализ защищенности;
- обнаружение вторжений;
- обеспечение безопасного доступа к сетям международного информационного обмена.

7.1. Идентификация и аутентификация

Управление доступом к ПДн осуществляется на основе принципа минимизации полномочий. Стандартным методом доступа является ролевой доступ, для чего определяются совокупности типов доступа - групповых прав и полномочий доступа пользователей (ролей), предоставляемых пользователям. Количество таких ролей ограниченно и подразумевает возможность эффективного управления. Назначение прав и полномочий конкретным пользователям осуществляется путем назначения им соответствующих ролей.

Каждый пользователь для получения соответствующих прав доступа при подключении к ИСПДн проходит процедуру идентификации, при этом используются уникальные признаки и имена. Стандартное средство проверки подлинности (аутентификации) – пароль. Для обеспечения более высокой надежности аутентификации возможно использование таких средств как токены, смарт-карты и другие носители аутентифицирующей информации.

7.2. Физическая защита

Физическая защита зданий, помещений, объектов и средств информатизации осуществляется путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации.

Размещение, специальное оборудование, охрана и организация режима в помещениях исключает возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.3. Регистрация и учет

В ИСПДн ведутся контрольные журналы, регистрирующие действия пользователей с ПДн. Установлены процедуры применения мониторинга действий с ПДн, а результаты действий пользователей регулярно просматриваются.

В целях повышения эффективности контроля действий возможных нарушителей возможно использование средств и методов активного мониторинга и аудита, направленных на выявление и регистрацию подозрительных действий в реальном масштабе времени.

7.4. Обеспечение целостности

В ТФОМС обеспечивается целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ.

Обеспечение целостности реализуется преимущественно операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

7.5. Антивирусная защита

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, осуществляющей обработку этой информации, применяются специальные средства антивирусной защиты, выполняющие:

- обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, реализующее обработку ПДн, а также на ПДн;
- обнаружение и удаление неизвестных вирусов;
- обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

7.6. Обеспечение безопасного межсетевого взаимодействия

Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами. Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Межсетевое экранирование обеспечивает:

- скрытие внутренней сетевой структуры ИСПДн;
- разрешение только такого входящего и исходящего трафика, который является необходимым для работы ИСПДн;
- блокирование любого входящего и исходящего трафика, не разрешенного явно.

7.7. Анализ защищенности

Анализ защищенности реализуется на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Для гарантии того, что СЗИ успешно выполняют свои функции, разрабатываются процедуры контроля изменений конфигураций СЗИ и сетевых устройств. Для выполнения этих процедур в информационно-телекоммуникационной среде создается система анализа защищенности, выполняющая следующие функции:

- контроль настроек сетевых устройств, СЗИ и программно-технического обеспечения ИСПДн;
- анализ уязвимостей настроек СЗИ, сетевых устройств или уязвимостей операционных систем или прикладного программного обеспечения.

7.8. Обнаружение вторжений

Обнаружение вторжений реализуется с использованием в составе СЗПДн программных и (или) программно-аппаратных средств (систем) обнаружения вторжений, использующих комбинированные методы обнаружения атак, включающие в себя сигнатурные методы и методы выявления аномалий.

7.9. Криптографическая защита

Для зашиты ПДн, передаваемых между ИСПДн по каналам связи, выходящим за пределы контролируемой зоны, используются защищенные каналы связи.

При использовании открытых и неконтролируемых каналов связи для защиты ПДн применяются средства криптографической защиты информации (далее – СКЗИ). Как раздельно, так и комплексно, используются следующие криптографические методы:

- шифрование, как средство обеспечения конфиденциальности информации;
- электронная цифровая подпись, как средство обеспечения подлинности и юридической значимости электронного документа;
- криптографическая аутентификация, как средство подтверждения санкционированности доступа субъекта к объекту;
- управление ключами, как необходимая составная часть систем с СКЗИ, которая применяется в целях изготовления, учета, распределения, хранения и уничтожения ключевых элементов.

7.10. Обеспечение безопасного доступа к сетям международного информационного обмена

Доступ ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к международной компьютерной сети «Интернет» допускается только с использованием специально предназначенных для этого средств защиты информации.

8 ПРИНЦИПЫ ОЦЕНКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В соответствии с принципом обязательности контроля выполняются следующие виды контроля эффективности системы защиты персональных данных:

- внутренний контроль;
- государственный контроль.

8.2. Внутренний контроль эффективности системы защиты ПДн осуществляется тФОМСс целью поддержания заданного уровня эффективности

СЗПДн, в соответствии с документированными методиками. Внутренний контроль включает:

- мониторинг состояния технических и программных средств, входящих в состав СЗПДн;
- контроль соблюдения требований по обеспечению безопасности ПДн (требований законодательства в области защиты ПДн, требований внутренних нормативно-методических и организационно-распорядительных документов ТФОМС, сформулированных на основе анализа рисков нарушения безопасности ПДн, договорных требований).

8.3.Оценка эффективности СЗПДн реализуется в виде аттестации соответствия требованиям по безопасности ПДн.

Аттестация производится по факту ввода в эксплуатацию ИСПДн. Ввод в эксплуатацию ИСПДн производится в соответствии с документально оформленными требованиями по безопасности ПДн (техническими условиями), разрабатываемыми ТФОМС в соответствии с требованиями законодательства и нормативно-методических документов федеральных органов исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

9 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ СУБЪЕКТА

9.1. Список работников ТФОМС, имеющих доступ к персональным данным, утверждается *приказом* директора ТФОМС.

9.2. Передача Персональных данных третьим лицам возможна только с согласия субъекта в письменной форме или без его согласия в случаях, предусмотренных законодательством РФ.

10. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

- 10.1. Система защиты персональных данных (СЗПДн), строится на основании:

- *«Отчета о результатах обследования информационной инфраструктуры»;*
- *«Перечня персональных данных, подлежащих защите»;*
- *«Актов классификации информационной системы персональных данных»;*
- *«Модели угроз безопасности персональных данных»;*
- Руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн. На основании анализа актуальных угроз безопасности ПДн описанного в «*Модели угроз безопасности персональных данных*», делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн, составляется *«План мероприятий по обеспечению защиты ПДн».*

10.2. Для каждой ИСПДн разрабатывается *«Разрешительная система допуска»* с описанием уровня полномочий доступа пользователей к защищаемым ресурсам и *«Технический паспорт ИСПДн»*, в котором отражается технологический процесс обработки персональных данных, перечень используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- Сервера приложений;
- СУБД.

10.3. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства управления доступом;
- средства регистрации и учета;
- средства защиты от НСД;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список включаются функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- осуществление обнаружений вторжений;
- осуществления анализа защищенности;
- обеспечение межсетевого экранирования.

Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения вносятся в *«Технический паспорт ИСПДн»*.

10.4. СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

10.5. Настройки применяемых средств защиты информации отражаются в *«Акте установки и настройки средств защиты»*. В случае необходимости внесения изменений настроек СЗИ, эти изменения фиксируются в приложении к указанному Акту с указанием даты внесения изменений.

10.6. С целью учета всех средств защиты информации используемых в ТФОМС ведется *«Журнал учета СЗИ, эксплуатационной и технической документации к ним»*

10.7. Порядок работы со средствами антивирусной защиты отражается в *«Инструкции по антивирусной защите».*

10.8. Порядок применения средств криптографической защиты информации отражается в *«Инструкции о порядке организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».*

Средства криптографической защиты учитываются в *«Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».*

Перечень лиц допущенных к работе с СКЗИ утверждается *приказом* директора ТФОМС.

10.9. Атрибуты доступа к средствам защиты информации и программным компонентам ИСПДн учитываются в *«Журнале учета атрибутов доступа».* Периодичность их смены отражается в *«Инструкции по парольной защите».*

10.10. В ТФОМС ведется учет всех электронных носителей персональных данных в *«Журнале учета носителей информации ПДн».*

10.11. Мероприятия и действия пользователей в случае возникновения инцидентов, повлекших нарушение целостности информации регламентированы в *«Инструкции по резервному копированию и восстановлению».*

10.12. Мероприятия по защите информации, содержащей персональные данные, при ее обработке без использования средств вычислительной техники регламентированы в *«Порядке неавтоматизированной обработки персональных данных».*

11. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

11.1. Все сотрудники ТФОМС, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

11.2. При вступлении в должность нового работника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работник должен быть ознакомлен под роспись с положениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

11.3. Работник, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

11.4. Работники должны следовать установленным процедурам поддержания режима безопасности ПДн при использовании паролей (если не используются технические средства аутентификации).

11.5. Работники ТФОМСа должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

11.6. Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

11.7. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ТФОМС, третьим лицам.

11.8. При работе с ПДн в ИСПДн работники ТФОМС обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

11.9. При завершении работы с ИСПДн работники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

11.10. Работники ТФОМС должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

11.11. Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему защиту информации.

11.12. В ИСПДн можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;
- Администратора безопасности;
- Пользователь ИСПДн.

11.13. Должностные обязанности пользователей ИСПДн отражаются в следующих документах:

- *«Инструкция администратора ИСПДн»;*
- *«Инструкция администратора безопасности ИСПДн»;*
- *«Инструкция пользователя ИСПДн».*

12. ПОРЯДОК РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ

12.1. Рассмотрение запросов субъектов персональных данных или их законных представителей осуществляется в порядке предусмотренном

«Регламентом рассмотрения запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных».

13. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА

13.1. Защита прав Субъекта, установленных настоящей Политикой и законодательством Российской Федерации, осуществляется в целях пресечения неправомерного использования Персональных данных, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

13.2. Работники ТФОМС, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, персонально несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

14. ЗАКЛЮЧИТЕЛЬНОЕ ПОЛОЖЕНИЕ

14.1. Изменения в настоящую Политику могут быть внесены директором ТФОМС.

14.2. Настоящая Политика обязательна для соблюдения всеми работниками ТФОМС.